

PATENTS

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re-application of

Yasutaka NAGAO

Serial No. (unknown)

Filed herewith

NETWORK TRAFFIC MONITORING  
SYSTEM AND MONITORING METHOD



CLAIM FOR FOREIGN PRIORITY UNDER 35 U.S.C. 119  
AND SUBMISSION OF PRIORITY DOCUMENT

Assistant Commissioner for Patents

Washington, D.C. 20231

Sir:

Attached hereto is a certified copy of applicant's corresponding patent application filed in Japan on January 19, 2000 under No. 2000-009605.

Applicant herewith claims the benefit of the priority filing date of the above-identified application for the above-entitled U.S. application under the provisions of 35 U.S.C. 119.

Respectfully submitted,

YOUNG & THOMPSON

By

Robert J. Patch  
Attorney for Applicant  
Registration No. 17,355  
745 South 23rd Street  
Arlington, VA 22202  
Telephone: 703/521-2297

January 18, 2001

後-池  
US

日 本 国 特 許 庁

PATENT OFFICE  
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

JP 09/761696  
01/18/01

出 願 年 月 日

Date of Application:

2000年 1月19日

出 願 番 号

Application Number:

特願2000-009605

出 願 人

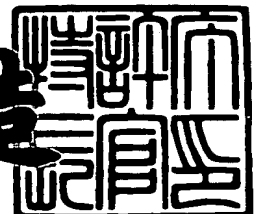
Applicant (s):

日本電気株式会社

2000年12月 8日

特許庁長官  
Commissioner,  
Patent Office

及川耕造



出証番号 出証特2000-3101720

【書類名】 特許願

【整理番号】 47201430

【提出日】 平成12年 1月19日

【あて先】 特許庁長官殿

【国際特許分類】 H04L 12/00

【発明者】

    【住所又は居所】 東京都港区芝五丁目7番1号 日本電気株式会社内

    【氏名】 長尾 泰孝

【特許出願人】

    【識別番号】 000004237

    【氏名又は名称】 日本電気株式会社

【代理人】

    【識別番号】 100088812

    【弁理士】

    【氏名又は名称】 ▲柳▼川 信

【手数料の表示】

    【予納台帳番号】 030982

    【納付金額】 21,000円

【提出物件の目録】

    【物件名】 明細書 1

    【物件名】 図面 1

    【物件名】 要約書 1

【ブルーフの要否】 要

【書類名】 明細書

【発明の名称】 ネットワークトラフィック監視システム及びそれに用いる監視方法

【特許請求の範囲】

【請求項1】 IP (Internet Protocol) パケット毎にサービス単位に応じて優先度を変えて転送するIPネットワークにおいてトラフィック監視を行うネットワークトラフィック監視システムであって、前記トラフィック監視を前記サービス単位及び前記IPネットワークのサブネットワーク単位で行う手段を有することを特徴とするネットワークトラフィック監視システム。

【請求項2】 IP (Internet Protocol) ネットワークを構築するIPルータがリンクによって相互に接続され、IPパケット転送の品質をクラス分けするDiffServ (differentiated service) プロトコルに基づいてサービスクラス分けされたIPパケットの転送を行うネットワークにおいてトラフィック監視を行うネットワークトラフィック監視システムであって、前記リンク上を転送されるIPパケットを監視する手段と、その監視で検出されたIPパケットの前記サービスクラスを表す値と送出元IPアドレス及び宛先IPアドレスから割り出される送出元サブネットワークアドレスと宛先サブネットワークアドレスとに基づいてトラフィックを分類する手段と、その分類されたトラフィックを前記サービスクラス毎及び前記IPネットワークのサブネットワーク毎に蓄積する手段とからなるトラフィックモニタ部を有することを特徴とするネットワークトラフィック監視システム。

【請求項3】 前記サービスクラスを表す値は、前記IPパケットのヘッダ内フィールドの一部に前記サービスクラスを表す値を記録するためのフィールドとして割り当てられたDSCP (DiffServ Code Point) を用いるようにしたことを特徴とする請求項2記載のネットワークトラフィック監視システム。

【請求項4】 前記サービスクラス毎及び前記サブネットワーク毎に蓄積さ

れたトラフィックデータに対して統計処理を施して前記トラフィックの表示と異常の監視とトレンドの把握とを行う監視マネージャを含むことを特徴とする請求項2または請求項3記載のネットワークトラフィック監視システム。

【請求項5】 前記監視マネージャは、前記サブネットワークのアドレス算出に必要なネットマスクを前記トラフィックモニタ部に供給するようにしたことを特徴とする請求項4記載のネットワークトラフィック監視システム。

【請求項6】 前記トラフィックモニタ部を前記IPルータ内に配置したことを特徴とする請求項2から請求項5のいずれか記載のネットワークトラフィック監視システム。

【請求項7】 前記トラフィックは、MIB (Management Information Base) の形式で蓄積するようにしたことを特徴とする請求項2から請求項6のいずれか記載のネットワークトラフィック監視システム。

【請求項8】 IP (Internet Protocol) パケット毎にサービス単位に応じて優先度を変えて転送するIPネットワークにおいてトラフィック監視を行うためのネットワークトラフィック監視方法であって、前記トラフィック監視を前記サービス単位及び前記IPネットワークのサブネットワーク単位で行うようにしたことを特徴とするネットワークトラフィック監視方法。

【請求項9】 IP (Internet Protocol) ネットワークを構築するIPルータがリンクによって相互に接続され、IPパケット転送の品質をクラス分けするDiffServ (differentiated service) プロトコルに基づいてサービスクラス分けされたIPパケットの転送を行うネットワークにおいてトラフィック監視を行うためのネットワークトラフィック監視方法であって、前記リンク上を転送されるIPパケットを監視し、その監視で検出されたIPパケットの前記サービスクラスを表す値と送出元IPアドレス及び宛先IPアドレスから割り出される送出元サブネットワークアドレスと宛先サブネットワークアドレスとに基づいてトラフィックを分類し、その分類されたトラフィックを前記サービスクラス毎及び前記IPネットワークのサブネットワーク毎に蓄積するようにしたことを特徴とするネットワークトラフィック

監視方法。

【請求項 1 0】 前記サービスクラスを表す値は、前記 I P パケットのヘッダ内フィールドの一部に前記サービスクラスを表す値を記録するためのフィールドとして割り当てられた D S C P ( D i f f s e r v C o d e P o i n t ) を用いるようにしたことを特徴とする請求項 9 記載のネットワークトラフィック監視方法。

【請求項 1 1】 前記サービスクラス毎及び前記サブネットワーク毎に蓄積されたトラフィックデータに対して統計処理を施して前記トラフィックの表示と異常の監視とトレンドの把握とを行うようにしたことを特徴とする請求項 9 または請求項 1 0 記載のネットワークトラフィック監視方法。

【請求項 1 2】 前記 I P ルータ内において、前記分類されたトラフィックを前記サービスクラス毎及び前記 I P ネットワークのサブネットワーク毎に蓄積するようにしたことを特徴とする請求項 9 から請求項 1 1 のいずれか記載のネットワークトラフィック監視方法。

【請求項 1 3】 前記トラフィックは、M I B ( M a n a g e m e n t I n f o r m a t i o n B a s e ) の形式で蓄積するようにしたことを特徴とする請求項 9 から請求項 1 2 のいずれか記載のネットワークトラフィック監視方法。

【発明の詳細な説明】

【 0 0 0 1 】

【発明の属する技術分野】

本発明はネットワークトラフィック監視システム及びそれに用いる監視方法に関し、特に大規模 I P ( I n t e r n e t P r o t o c o l ) ネットワークにおけるトラフィック監視方法に関する。

【 0 0 0 2 】

【従来の技術】

従来、トラフィック監視手法においては、一般に、I P ヘッダ内から送信元 I P アドレスと宛先 I P アドレスとを読み出し、これらの I P アドレスペアと 4 層宛先ポート番号とから識別される上位アプリケーション種別によって集計を行って

いる。

【0003】

一方、IETF (Internet Engineering Task Force) によって新たなプロトコルとして、従来平等に転送されていたIPパケットに対して転送の優先度を設け、サービスに差別を設けるという技術が議論されるようになっていく。これがDiffserv (differentiated service) プロトコルである。

【0004】

Diffservプロトコルに対応した端末や、Diffservサービスの境界となるルータでは、転送するIPパケットの送信元IPアドレスや宛先IPアドレス、使用するポート番号等によってパケットを数種類 (IETFのRFC 2475では、14種のクラス) のサービスクラスに分類し、DSCP (Diffserv Code Point) としてIPヘッダ内に情報を埋め込んでパケット転送を行う。

【0005】

Diffservプロトコルをサポートしたルータは、IPヘッダ内に埋め込まれたDSCPの値を読み込んで優先レベルを判断し、転送方法を決定するというアーキテクチャである。これによって、IPパケットはクラス毎に分類された数種類のフローとして扱われ、特定のホストのIPパケットの廃棄率を低く設定したり、特定のアプリケーションパケットを低遅延で転送させたりすることが可能となる。

【0006】

【発明が解決しようとする課題】

以上のようなネットワークに対し、従来のトラフィック監視方式においては、4層プロトコルのポート番号によってアプリケーション毎に総トラフィック量を分類しているため、Diffservプロトコルによって生ずる転送優先度を把握することができず、ネットワークがどのようなサービスに割り当てられているかを監視することができない。

【0007】

また、End-to-Endの端末同士でやりとりされるトラフィック量を分類しているので、ネットワークの規模が大きくなるにつれて扱うIPアドレス数が増加し、トラフィックモニタ部のメモリ容量圧迫や管理ネットワークへ負荷が増大するため、大規模ネットワークに対応しきれない。

## 【0008】

さらに、IPsec (security architecture for internet protocol) やIPoverIPのようなプロトコルを用いたネットワークでは4層プロトコルのポート番号を監視することができなくなるため、トラフィックをアプリケーション毎に分類することができない。

## 【0009】

そこで、本発明の目的は上記の問題点を解消し、Diffservプロトコルを用いたIPネットワークにおいてネットワークの挙動を左右するサービス分布を把握することができ、大規模ネットワークにも対応することができるネットワークトラフィック監視システム及びそれに用いる監視方法を提供することにある。

## 【0010】

## 【課題を解決するための手段】

本発明によるネットワークトラフィック監視システムは、IP (Internet Protocol) パケット毎にサービス単位に応じて優先度を変えて転送するIPネットワークにおいてトラフィック監視を行うネットワークトラフィック監視システムであって、前記トラフィック監視を前記サービス単位及び前記IPネットワークのサブネットワーク単位で行う手段を備えている。

## 【0011】

本発明による他のネットワークトラフィック監視システムは、IP (Internet Protocol) ネットワークを構築するIPルータがリンクによって相互に接続され、IPパケット転送の品質をクラス分けするDiffserv (differentiated service) プロトコルに基づいてサービスクラス分けされたIPパケットの転送を行うネットワークにおいてトラフィック監視を行うネットワークトラフィック監視システムであって、前記リンク



上を転送されるIPパケットを監視する手段と、その監視で検出されたIPパケットの前記サービスクラスを表す値と送出元IPアドレス及び宛先IPアドレスから割り出される送出元サブネットワークアドレスと宛先サブネットワークアドレスとに基づいてトラフィックを分類する手段と、その分類されたトラフィックを前記サービスクラス毎及び前記IPネットワークのサブネットワーク毎に蓄積する手段とからなるトラフィックモニタ部を備えている。

#### 【0012】

本発明によるネットワークトラフィック監視方法は、IP (Internet Protocol) パケット毎にサービス単位に応じて優先度を変えて転送するIPネットワークにおいてトラフィック監視を行うためのネットワークトラフィック監視方法であって、前記トラフィック監視を前記サービス単位及び前記IPネットワークのサブネットワーク単位で行うようにしている。

#### 【0013】

本発明による他のネットワークトラフィック監視方法は、IP (Internet Protocol) ネットワークを構築するIPルータがリンクによって相互に接続され、IPパケット転送の品質をクラス分けするDiffServ (differentiated service) プロトコルに基づいてサービスクラス分けされたIPパケットの転送を行うネットワークにおいてトラフィック監視を行うためのネットワークトラフィック監視方法であって、前記リンク上を転送されるIPパケットを監視し、その監視で検出されたIPパケットの前記サービスクラスを表す値と送出元IPアドレス及び宛先IPアドレスから割り出される送出元サブネットワークアドレスと宛先サブネットワークアドレスとに基づいてトラフィックを分類し、その分類されたトラフィックを前記サービスクラス毎及び前記IPネットワークのサブネットワーク毎に蓄積するようにしている。

#### 【0014】

すなわち、本発明のネットワークトラフィック監視システムは、インターネットやイントラネットに代表されるIPネットワークにおいて、トラフィック監視をサービス単位及びサブネットワーク単位で行うことによって収集するデータを集

約させてデータ量を削減し、大規模ネットワーク監視に適した監視システムを提供することを特徴としている。

## 【 0 0 1 5 】

より具体的に、本発明のネットワークトラフィック監視システムは、IPネットワークを構築するIPルータであるNE（ネットワークエレメント）がリンクによって相互に接続されており、Diffserv（differentiated service）プロトコルに基づいてクラス分けされたIPパケットの転送を行っている。

## 【 0 0 1 6 】

DiffservプロトコルはIETFによって議論されているIPパケット転送の品質をクラス分けするプロトコルであり、IPヘッダ内のフィールドの一部をサービスクラスを表すDSCP（Diffserv Code Point）を記録するためのフィールドとして割り当て、このフィールドに設定される14種のDSCP値にしたがってパケット毎に優先度を変えて転送するという方式である。

## 【 0 0 1 7 】

トラフィックモニタ部はリンク上を転送されるIPパケットを監視し、つまりパケットをキャプチャし、サービスクラスを表すDSCPの値と、送出元IPアドレス及び宛先IPアドレスから割り出される送出元サブネットワークアドレスと、宛先サブネットワークアドレスとに基づいてトラフィックを分類し、内部メモリに蓄積するための装置である。

## 【 0 0 1 8 】

蓄積されたトラフィックデータはSNMP（Simple Network Management Protocol）等を用いて監視マネージャへ転送されて統計処理が施され、トラフィックの表示・異常の監視・トレンドの把握等に用いられる。監視マネージャではサブネットワークアドレス算出に必要なネットマスクを入力するためのユーザインタフェースも提供する。

## 【 0 0 1 9 】

このようにして、本発明ではトラフィック監視の粒度としてサービスクラス毎

及びサブネットワーク毎に集計を行っているので、ネットワーク上の全端末同士で交換されるトラフィック情報を全アプリケーション毎に把握する代わりに、サブネットワーク毎・サービスクラス毎のトラフィックとして集約させた形で捉えることが可能となり、トラフィックモニタ部に必要なメモリ量を節約したり、監視マネージャへの通信量を低くすることが可能となる。

## 【 0 0 2 0 】

また、このようにして得られる集約されたトラフィックデータは、特に大規模ネットワークにおいてトラフィック管理をマクロ的に行う場合に有効な情報であることは言うまでもない。

## 【 0 0 2 1 】

よって、D i f f s e r v プロトコルを用いた IP ネットワークにおいて、トラフィック監視の集計をサービス単位及びサブネットワーク単位で収集することで情報を集約させて監視することによって、ネットワークの挙動を左右するサービス分布を把握し、かつ大規模ネットワークにも対応可能となる。

## 【 0 0 2 2 】

## 【発明の実施の形態】

次に、本発明の実施例について図面を参照して説明する。図 1 は本発明の一実施例によるネットワークトラフィック監視システムの構成を示すブロック図である。図 1 において、NE（ネットワークエレメント）1，2 は IP ネットワークを構築する IP ルータであり、リンク 1 0 0 によって相互に接続されており、D i f f s e r v（d i f f e r e n t i a t e d s e r v i c e）プロトコルに基づいてクラス分けされた IP パケットの転送を行っている。

## 【 0 0 2 3 】

D i f f s e r v プロトコルは I E T F によって議論されている IP パケット転送の品質をクラス分けするプロトコルであり、IP ヘッダ内のフィールドの一部をサービスクラスを表す D S C P（D i f f s e r v C o d e P o i n t）を記録するためのフィールドとして割り当て、このフィールドに設定される 1 4 種の D S C P 値にしたがって、パケット毎に優先度を変えて転送するという方式である。

## 【 0 0 2 4 】

トラフィックモニタ部（プローブ）3はリンク100上を転送されるIPパケットを監視し、つまりパケットをキャプチャし、サービスクラスを表すDSCPの値と、送出元IPアドレス及び宛先IPアドレスから割り出される送出元サブネットワークアドレスと、宛先サブネットワークアドレスとに基づいてトラフィックを分類し、内部メモリ（図示せず）に蓄積するための装置である。

## 【 0 0 2 5 】

蓄積されたトラフィックデータはSNMP（Simple Network Management Protocol）等を用いて監視マネージャ4へ転送されて統計処理が施され、トラフィックの表示・異常の監視・トレンドの把握等に用いられる。監視マネージャ4ではサブネットワークアドレス算出に必要なネットマスクを入力するためのユーザインタフェースも提供する。

## 【 0 0 2 6 】

このようにして、本実施例ではトラフィック監視の粒度としてサービスクラス毎及びサブネットワーク毎に集計を行っているので、図示せぬネットワーク上の全端末同士で交換されるトラフィック情報を全アプリケーション毎に把握する代わりに、サブネットワーク毎・サービスクラス毎のトラフィックとして集約させた形で捉えることができ、トラフィックモニタ部3に必要なメモリ量を節約したり、監視マネージャ4への通信量を低くすることができる。

## 【 0 0 2 7 】

また、このようにして得られる集約されたトラフィックデータは、特に大規模ネットワークにおいてトラフィック管理をマクロ的に行う場合に有効な情報である。

## 【 0 0 2 8 】

図2は図1のトラフィックモニタ部3の構成を示すブロック図である。図2において、トラフィックモニタ部3はインタフェース部31と、抽出部32と、回析部33と、制御部34と、メモリ部（MIB：Management Information Base）35と、SNMPエージェント36とから構成されている。

## 【 0 0 2 9 】

インタフェース部 3 1 はネットワークリンク 1 0 0 と接続され、IP パケットのキャプチャを行い、物理層及びデータリンク層の終端を行う部分である。抽出部 3 2 は下位層の終端が行われた IP ヘッダから、集計に必要となる D S C P と送出元 IP アドレスと宛先 IP アドレスとをそれぞれ抽出する。

## 【 0 0 3 0 】

解析部 3 3 は抽出された情報と制御部 3 4 から受け渡されるネットマスクとからサービスクラス毎及びサブネットワーク毎のトラフィックを集計し、M I B の形式でメモリ部 3 5 に蓄積を行う部分である。制御部 3 4 はサブネットワークアドレス算出のためのネットマスクを監視マネージャ 4 から S N M P エージェント 3 6 経由で設定したり、トラフィックモニタ部 3 全体の動作制御を行う部分である。S N M P エージェント 3 6 はトラフィックモニタ部 3 と監視マネージャ 4 との間のデータ交換に用いられる。

## 【 0 0 3 1 】

監視マネージャ 4 は S N M P プロトコルを用いてトラフィックモニタ部 3 にネットマスクを設定したり、定期的にトラフィックモニタ部 3 内のメモリ部 3 5 に M I B の形式で保存された収集データにアクセスを行って、このデータをさらに統計・加工処理してトラフィック状態を表示したり、データを蓄積して異常状態の監視やトレンドの把握を行う装置である。

## 【 0 0 3 2 】

以上、本実施例の構成について述べたが、監視マネージャ 4 は当業者にとってよく知られており、また本発明とは直接関係しないので、その詳細な構成及び動作についての説明は省略する。

## 【 0 0 3 3 】

図 3 は図 2 の抽出部 3 2 へ送られるヘッダ情報の詳細を示す図である。図 3 ( a ) は I P v 4 ( I n t e r n e t   P r o t o c o l   v e r s i o n   4 ) フォーマットのヘッダ情報を示し、図 3 ( b ) は I P v 6 ( I n t e r n e t   P r o t o c o l   v e r s i o n   6 ) フォーマットのヘッダ情報を示している。

## 【 0 0 3 4 】

図 4 は図 2 の解析部 3 3 にて行う集計動作を説明するための図である。これら図 1 ～図 4 を参照して本発明の一実施例によるネットワークトラフィック監視システムの動作について説明する。

## 【 0 0 3 5 】

まず、トラフィック監視に先立ち、監視マネージャ 4 からトラフィックモニタ部 3 に対してサブネットワーク算出に用いるネットマスクが設定される。ネットマスクは IP アドレスのホストアドレスを隠蔽するためのビット列であり、設定はビットを指定しても良いし、例えば ( 2 5 5 . 2 5 5 . 2 5 5 . 0 ) や ( 2 5 5 . 2 5 5 . 0 . 0 ) 、 ( 2 5 5 . 0 . 0 . 0 ) といったアドレスの形式としても良い。トラフィックモニタ部 3 はこれを制御部 3 4 に記録しておく。

## 【 0 0 3 6 】

次に、トラフィックモニタ部 3 がリンク 1 0 0 上を流れる IP パケットを受信した場合、インタフェース部 3 1 では受信した IP パケットの物理層及びデータリンク層を終端し、ヘッダ情報を抽出部 3 2 へ送る。

## 【 0 0 3 7 】

ここで、抽出部 3 2 へ送られるヘッダ情報の詳細を図 3 に示す。図 3 ( a ) は IPv 4 フォーマットのヘッダ情報を示しており、IP ヘッダの先頭から 2 バイト目に T O S ( T y p e o f S e r v i c e ) フィールド 1 1 が、3 バイト目に L e n g t h フィールド 1 3 が、1 3 バイト目に宛先 IP アドレスフィールド 1 4 が、1 7 バイト目に送出元 IP アドレスフィールド 1 5 がそれぞれ位置している。D S C P は T O S フィールド 1 1 にマッピングされている。

## 【 0 0 3 8 】

また、図 3 ( b ) は IPv 6 フォーマットのヘッダ情報を示しており、5 バイト目に T r a f f i c C l a s s フィールド 1 2 が、5 バイト目に L e n g t h フィールド 1 3 が、9 バイト目に宛先 IP アドレスフィールド 1 4 が、2 5 バイト目に送出元 IP アドレスフィールド 1 5 がそれぞれ位置している。D S C P は T r a f f i c C l a s s フィールド 1 2 にマッピングされている。抽出部 3 2 はこれらの情報を読取って解析部 3 3 へと送る。

## 【 0 0 3 9 】

解析部 3 3 は制御部 3 4 から受け渡されたネットマスクと、IP ヘッダから抽出された宛先 IP アドレス及び送出元 IP アドレスとの和をとることによって、宛先サブネットワークと送出元サブネットワークとを算出し、このサブネットワークのペアと、同様に IP ヘッダから抽出された D S C P 値（すなわち、サービスクラス）毎にエントリを作成し、該当エントリについて L e n g t h フィールド 1 3 で示された IP パケット長、エントリを確認した回数（すなわち、該当 IP パケットの受信回数）それぞれの累積を、メモリ部 3 5 に M I B 情報として蓄積する。

## 【 0 0 4 0 】

次に、解析部 3 3 にて行う集計動作について例を挙げて説明する。現在、監視マネージャ 4 からトラフィックモニタ部 3 に、( 2 5 5 . 2 5 5 . 0 . 0 ) というネットマスクが設定されているものとする。

## 【 0 0 4 1 】

この状態において、トラフィックモニタ部 3 が送出元 IP アドレス ( 1 0 . 2 4 . 3 2 . 1 0 1 ) から宛先アドレス ( 2 0 . 3 2 . 5 2 . 2 1 1 ) に対して送られた D S C P 値 ( 1 0 1 1 1 0 ) のパケット長 L の IP パケットを受信したとする。

## 【 0 0 4 2 】

このとき、トラフィックモニタ部 3 の解析部 3 3 では、図 4 に示すようなエントリ 2 1 a を作成する。作成されたエントリ 2 1 a はパケット長 L とともにメモリ部 3 5 内にレンジスカウンタ 3 5 b、エントリカウンタ 3 5 c とともに 1 つのレコード 3 5 a として格納される。

## 【 0 0 4 3 】

エントリカウンタ 3 5 c はレコード 3 5 a が生成された時に「1」であり、該当エントリが収集される毎に 1 ずつインクリメントされるカウンタで、すなわち該当 IP パケット通信個数を表す。レンジスカウンタ 3 5 b はキャプチャされる毎にパケットレンジスが加算されるカウンタで、すなわち該当 IP パケットの通信オクテット数を表す。

## 【0044】

続いて、送出元IPアドレス（10．24．33．10）から宛先アドレス（20．32．52．200）に対して送られたDSCP値（101110）のパケット長MのIPパケットを受信したとする。このパケットのエントリは先に作られたエントリ21aのものと一致するので、エントリカウンタ35cは「2」となり、レングスカウンタ35bは「L+M」となる。

## 【0045】

また、送出元IPアドレス（10．24．33．10）から宛先アドレス（20．32．52．．211）に対して送られたDSCP値（001010）のパケット長MのIPパケットを受信したとする。この場合、サブネットアドレスは先に送られているIPパケットと一致するが、DSCPが異なるため、新たなエントリ21bとしてメモリ部35に格納される。

## 【0046】

このように、従来方式のように個々のIPアドレスでエントリを作成した場合、n台のホストがある状況では最大で $n \times (n - 1)$ 個のエントリを作成しなければならず、また4層ポート番号によってプロトコルの識別を行っているため、使用されるポート番号の個数に比例したエントリがさらに必要となる。

## 【0047】

一方、本実施例のようにサービス毎・サブネットワーク毎に集計を行えば、プロトコルは14種のサービスのいずれかに分類されるため、サブネットワークがm個（ $m < n$ ）である場合、エントリは最大でも $m \times (m - 1) \times 14$ 個だけ作成されることになる。

## 【0048】

よって、本実施例ではサービス毎・サブネットワーク毎に集計を取っているので、プロトコル毎・End-to-Endの端末毎に情報を蓄積する場合に比べて情報量が少なくなり、トラフィックモニタ部3のメモリを節約することができる。

## 【0049】

また、本実施例ではサービス毎・サブネットワーク毎に集計を取っているので



、大規模ネットワークに対しても監視の適用が可能となる。エントリ数は $n$ や $m$ の2乗に比例するので、 $n$ と $m$ との差が大きければ大きいほど、つまり大規模ネットワークほど効果が大きく表れる。

## 【0050】

さらに、本実施例ではサービス毎・サブネットワーク毎に集計を取っているの  
で、監視マネージャ4へ転送する情報も少なくなるため、管理ネットワーク上の  
通信負荷を削減することができる。

## 【0051】

さらにまた、抽出する情報が全てIPヘッダ上にあるため、IPsec (se  
curity architecture for internet prot  
ocol) のESP (Encapsulation Security Pay  
load) やIPoverIPのようなカプセル化プロトコルを用いたネットワ  
ークに対しても、サービスレベルでのトラフィック監視が可能となる。

## 【0052】

従来方式では上記のIPsecやIPoverIPプロトコルが用いられたネ  
ットワークにおいて、4層ポート番号が暗号化されたり、ヘッダ先頭からの位置  
が変化してしまうので、情報を抽出することができず、トラフィックをプロトコ  
ル毎に分類することができない。

## 【0053】

一方、本実施例のようにDSCPに基づいたサービス毎のトラフィック集計は  
カプセル化外部のIPヘッダ内にその情報が含まれるため、その監視を行うこと  
ができる。また、DiffServプロトコルを用いたネットワークにおいては  
、各種アプリケーションによって分類されたトラフィック情報よりも、転送優先  
度に基づいて分類されたトラフィック情報の方が、ネットワークのQoS (Q u  
a l i t y o f S e r v i c e) を端的に表現することができるため、付加  
価値の高い情報として扱うことができる。本実施例では以上の効果から、監視シ  
ステム全体としての監視性能向上が見込まれる。

## 【0054】

上記の監視マネージャ4からトラフィックモニタ部3に設定するネットマスク

は自由に設定可能であるため、(255. 255. 255. 255)のようなマスクを設定した場合、サブネットワークアドレスがホストIPアドレスと等しくなり、従来のようなEnd-to-End毎のトラフィック監視も可能となる。

## 【0055】

図5は本発明の他の実施例によるルータの構成を示すブロック図である。図5においては本発明の他の実施例によるルータ5内部にトラフィックモニタ部51を組込んだ例を示している。

## 【0056】

ルータ5のインタフェース#1～#nからなるインタフェース部31に到着したパケットのヘッダ情報はフォワーディングエンジン部52へ転送され、宛先IPアドレスからハードウェア的に送出先が検索される。このヘッダ情報を抽出部32にもフォワーディングエンジン部52と同様に受け渡すことによって、ルータ5のインタフェース部31に関わらずトラフィックを収集することができるようになる。よって、ノードにおけるトラフィック監視が可能となる。

## 【0057】

この形態において、(0. 0. 0. 0)のようなマスクを設定した場合には、図示せぬネットワーク内のサービス分布(どのノードにどのサービスが集中しているか等)を把握することも可能となる。

## 【0058】

また、上記の形態において、トラフィックモニタ部51と監視マネージャ(図示せず)との間の通信にCOPS(Common Open Policy System)プロトコルを用いた場合には、トラフィックモニタ51部と監視マネージャ部との信頼性の高い通信や、監視ポリシーの設定を実現することができる。COPSプロトコルを利用する場合にはポリシー受け渡しのためのクライアントタイプを予め設定しなければならないが、トラフィックモニタのためのクライアントタイプはIETFでも決定はされていないため、新たなクライアントタイプとして登録を行う。

## 【0059】

## 【発明の効果】

以上説明したように本発明によれば、IP (Internet Protocol) パケット毎にサービス単位に応じて優先度を変えて転送するIPネットワークにおいてトラフィック監視を行うネットワークトラフィック監視システムにおいて、トラフィック監視をサービス単位及びIPネットワークのサブネットワーク単位で行うことによって、DiffServプロトコルを用いたIPネットワークにおいてネットワークの挙動を左右するサービス分布を把握することができ、大規模ネットワークにも対応することができるという効果がある。

【図面の簡単な説明】

【図1】

本発明の一実施例によるネットワークトラフィック監視システムの構成を示すブロック図である。

【図2】

図1のトラフィックモニタ部の構成を示すブロック図である。

【図3】

(a) はIPv4フォーマットのヘッダ情報を示す図、(b) はIPv6フォーマットのヘッダ情報を示す図である。

【図4】

図2の解析部にて行う集計動作を説明するための図である。

【図5】

本発明の他の実施例によるルータの構成を示すブロック図である。

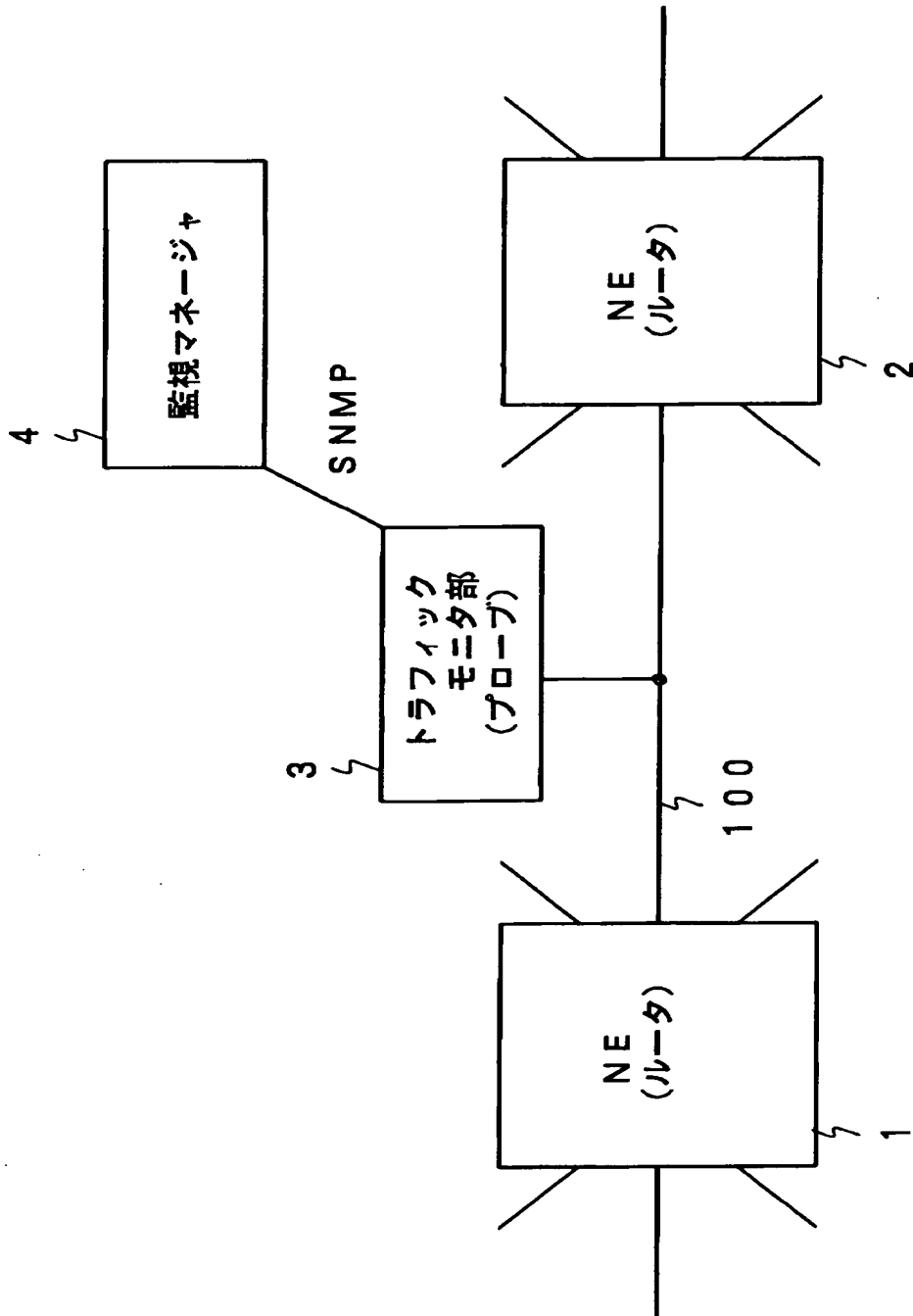
【符号の説明】

- 1, 2 NE
- 3, 5 1    トラフィックモニタ部
- 4    監視マネージャ
- 5    ルータ
- 1 1    TOSフィールド
- 1 2    Traffic Classフィールド
- 1 3    Lengthフィールド
- 1 4    宛先IPアドレスフィールド

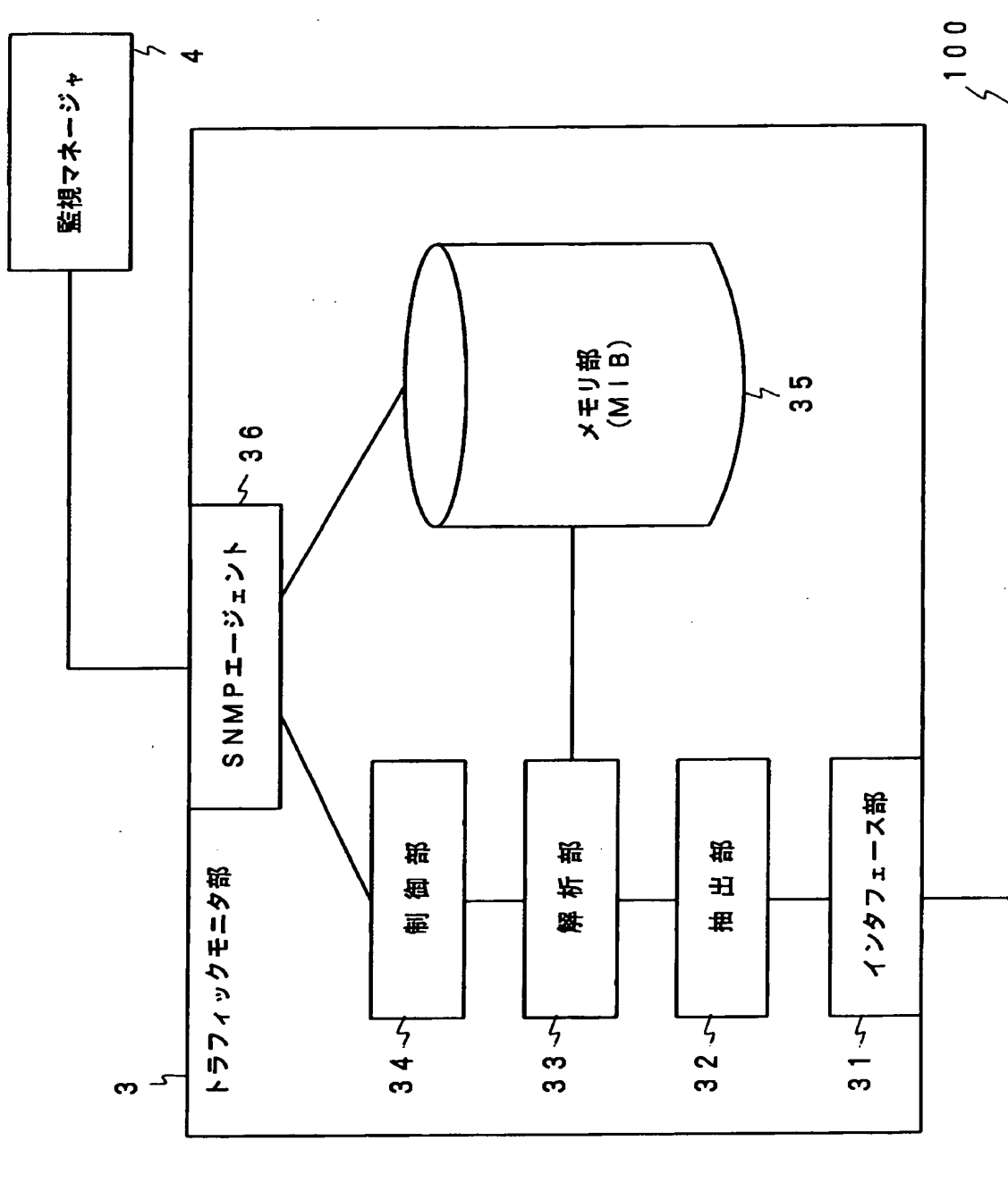
- 1 5 送出元 I P アドレスフィールド
- 2 1 a, 2 1 b エントリ
  - 3 1 インタフェース部
  - 3 2 抽出部
  - 3 3 回析部
  - 3 4 制御部
  - 3 5 メモリ部
  - 3 5 a レコード
  - 3 5 b レングスカウンタ
  - 3 5 c エントリカウンタ
  - 3 6 S N M P エージェント
- 5 2 フォワーディングエンジン部
- 1 0 0 リンク

【書類名】 図面

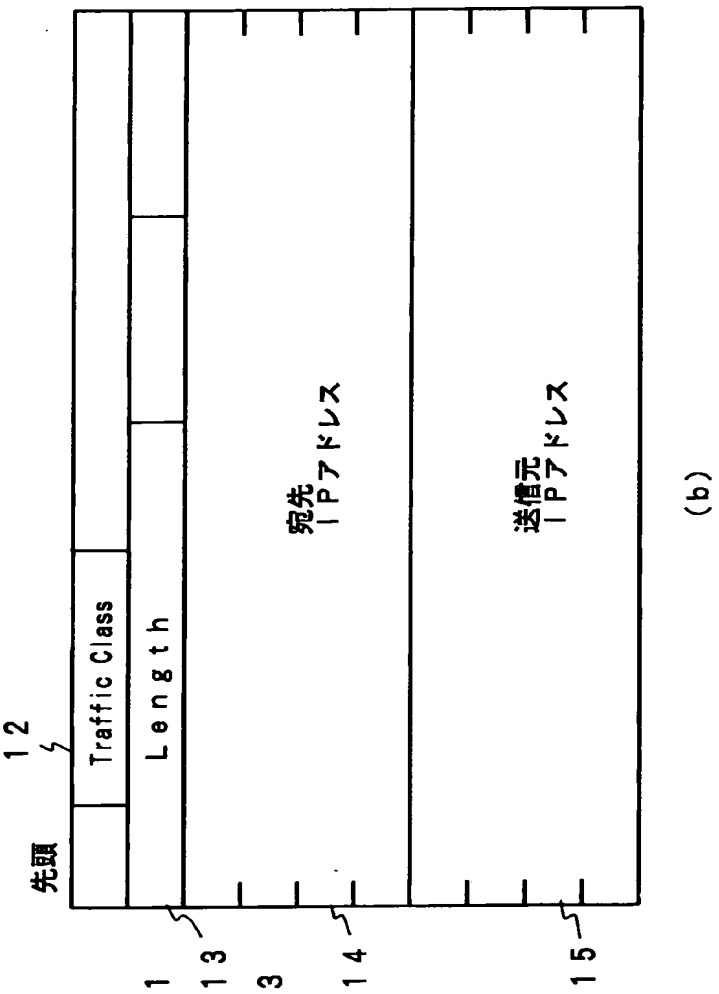
【図1】



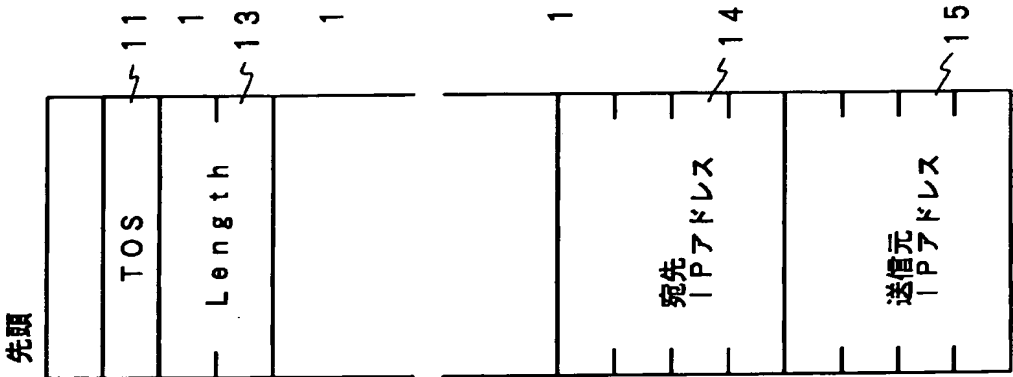
【図 2】



【図 3】

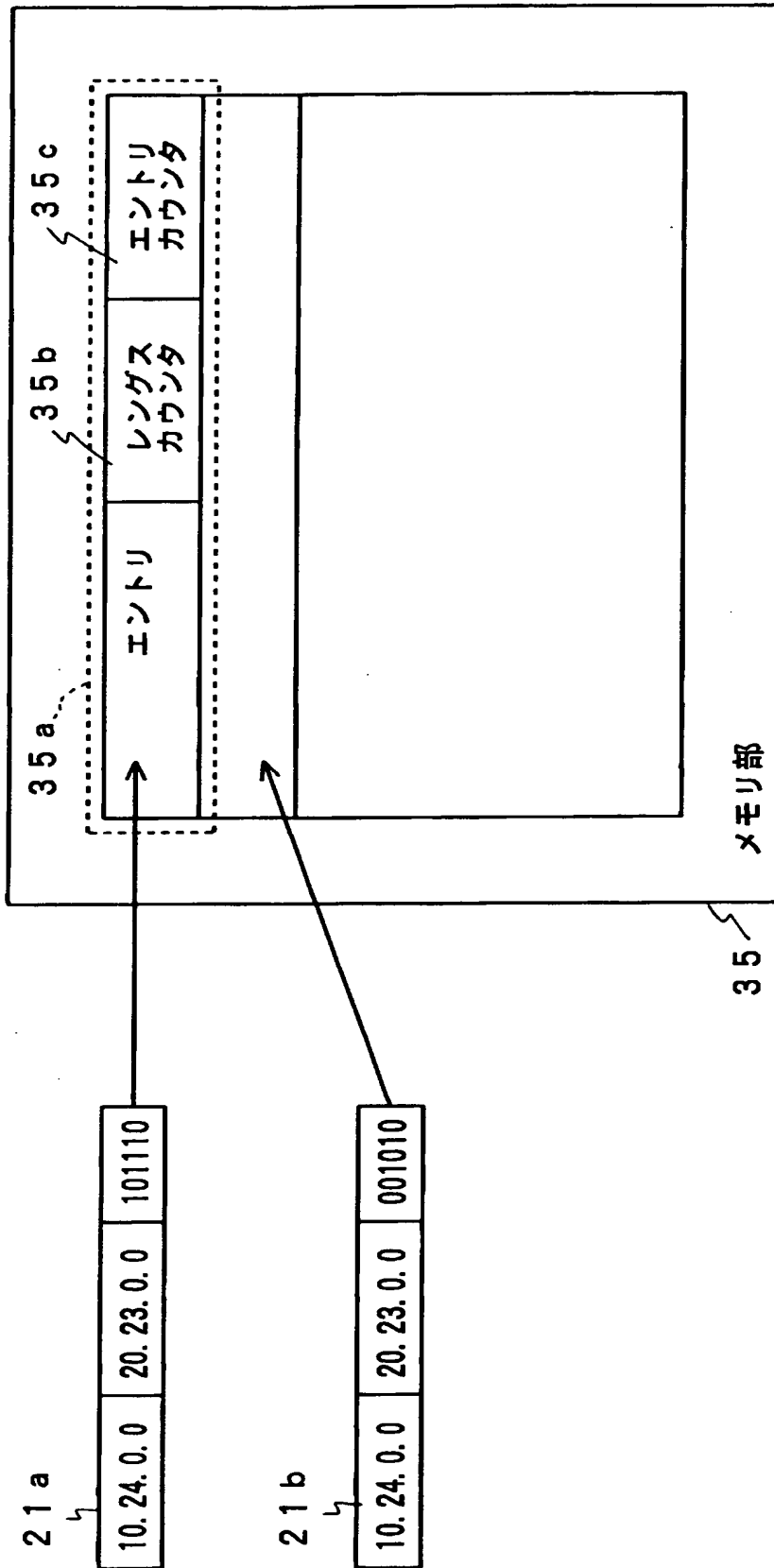


(b)



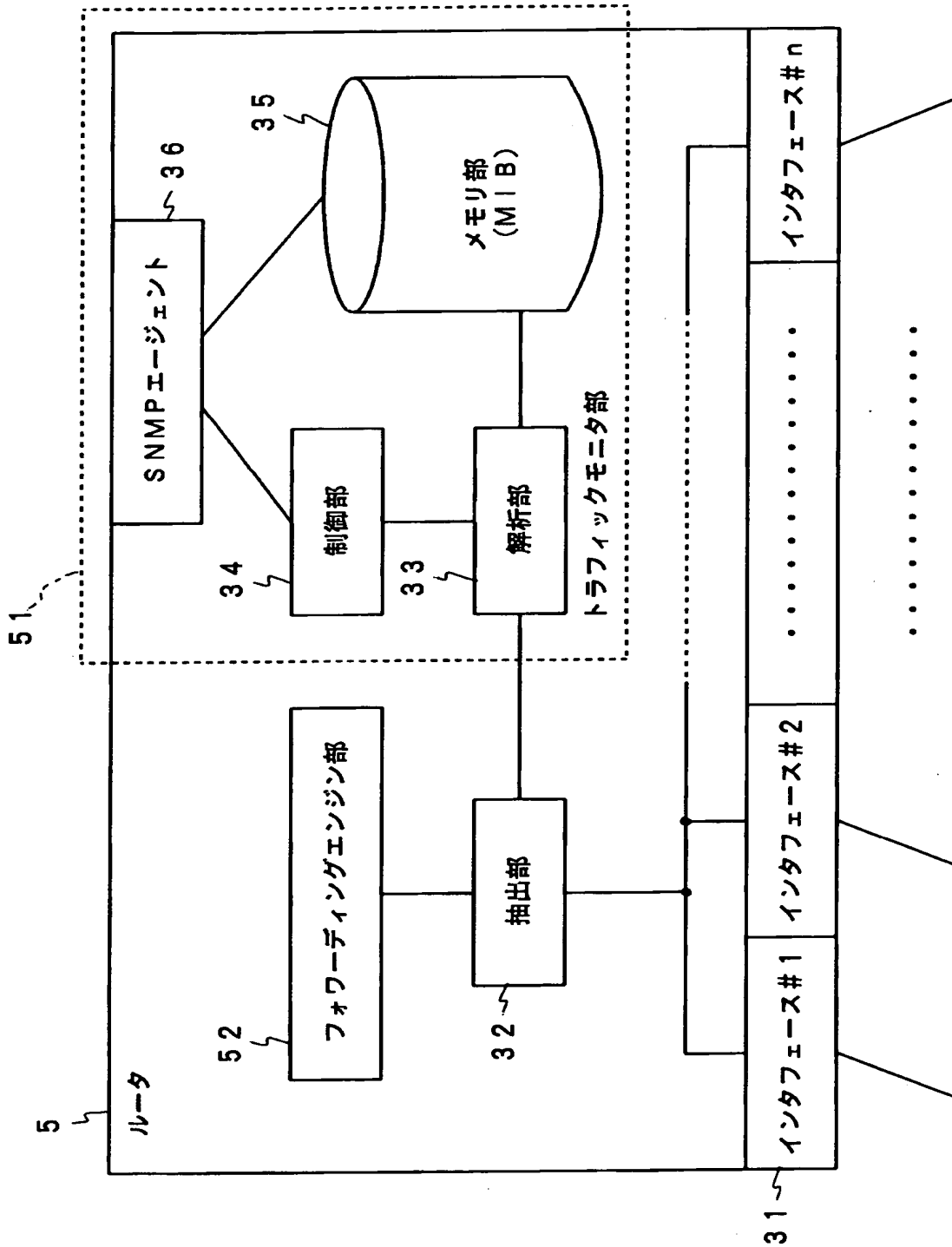
(a)

【図 4】





【図 5】



【書類名】 要約書

【要約】

【課題】 D i f f s e r v プロトコルを用いた I P ネットワークにおいてネットワークの挙動を左右するサービス分布を把握し、大規模ネットワークにも対応可能なネットワークトラフィック監視システムを提供する。

【解決手段】 インタフェース部 3 1 は I P パケットのキャプチャを行い、物理層及びデータリンク層の終端を行う。抽出部 3 2 は I P ヘッダから集計に必要な D S C P と送出元 I P アドレスと宛先 I P アドレスとを抽出する。解析部 3 3 は抽出された情報とネットマスクとからサービスクラス毎及びサブネットワーク毎のトラフィックを集計し、M I B の形式でメモリ部 3 5 に蓄積する。制御部 3 4 はサブネットワークアドレス算出のためのネットマスクを監視マネージャ 4 から S N M P エージェント 3 6 経由で設定し、トラフィックモニタ部 3 全体の動作制御を行う。

【選択図】 図 2

出 願 人 履 歴 情 報

識別番号 [000004237]

1. 変更年月日	1990年 8月29日
[変更理由]	新規登録
住 所	東京都港区芝五丁目7番1号
氏 名	日本電気株式会社